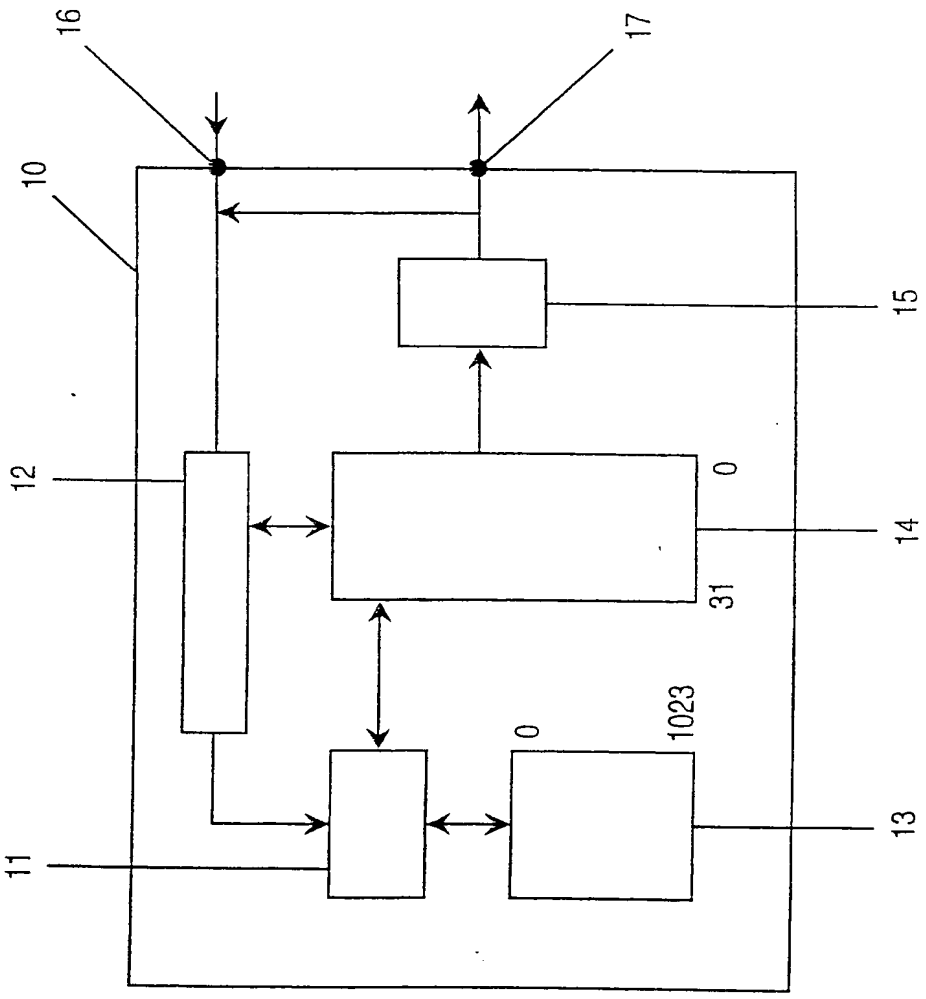

Fig.1

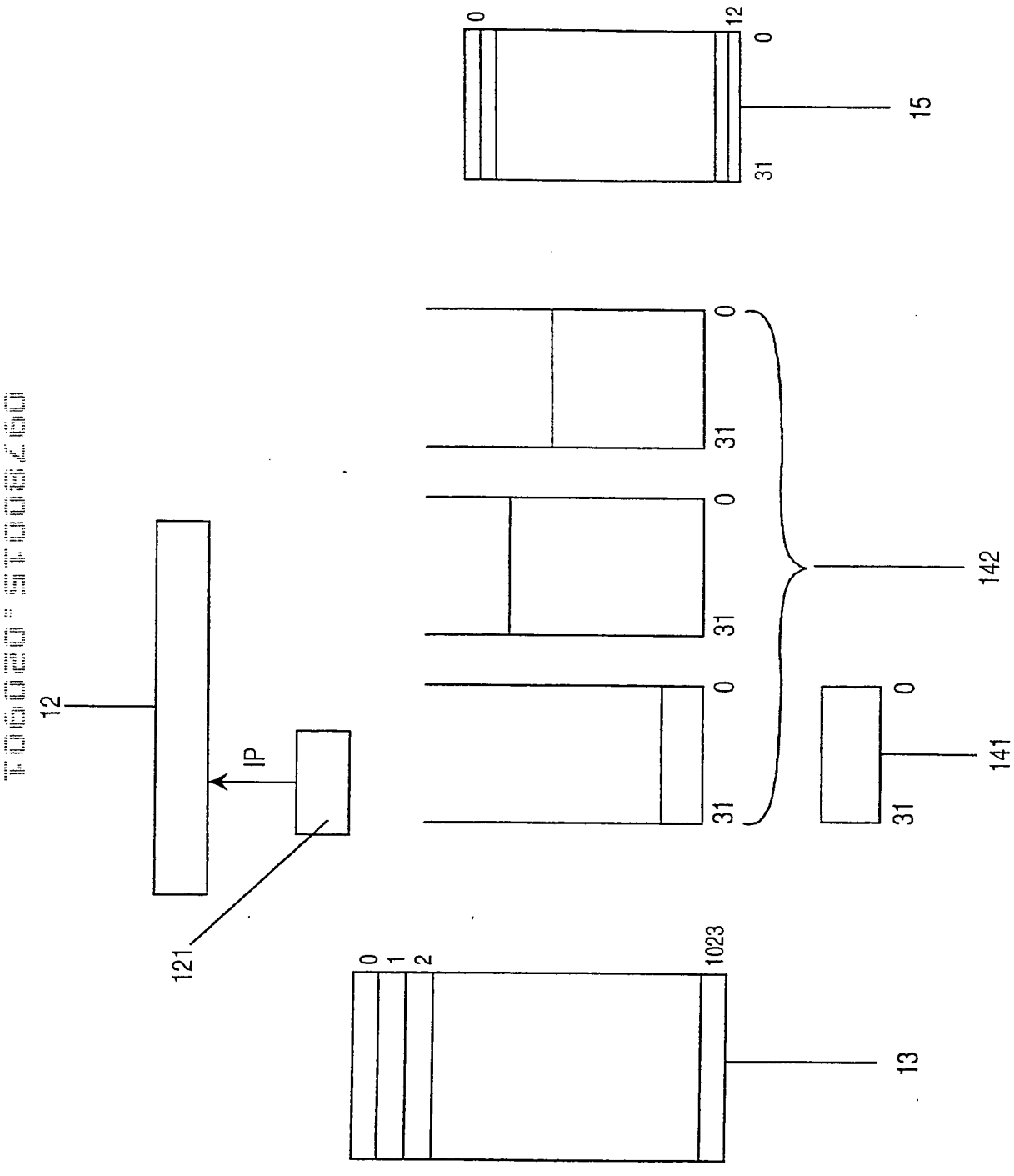

Fig.2

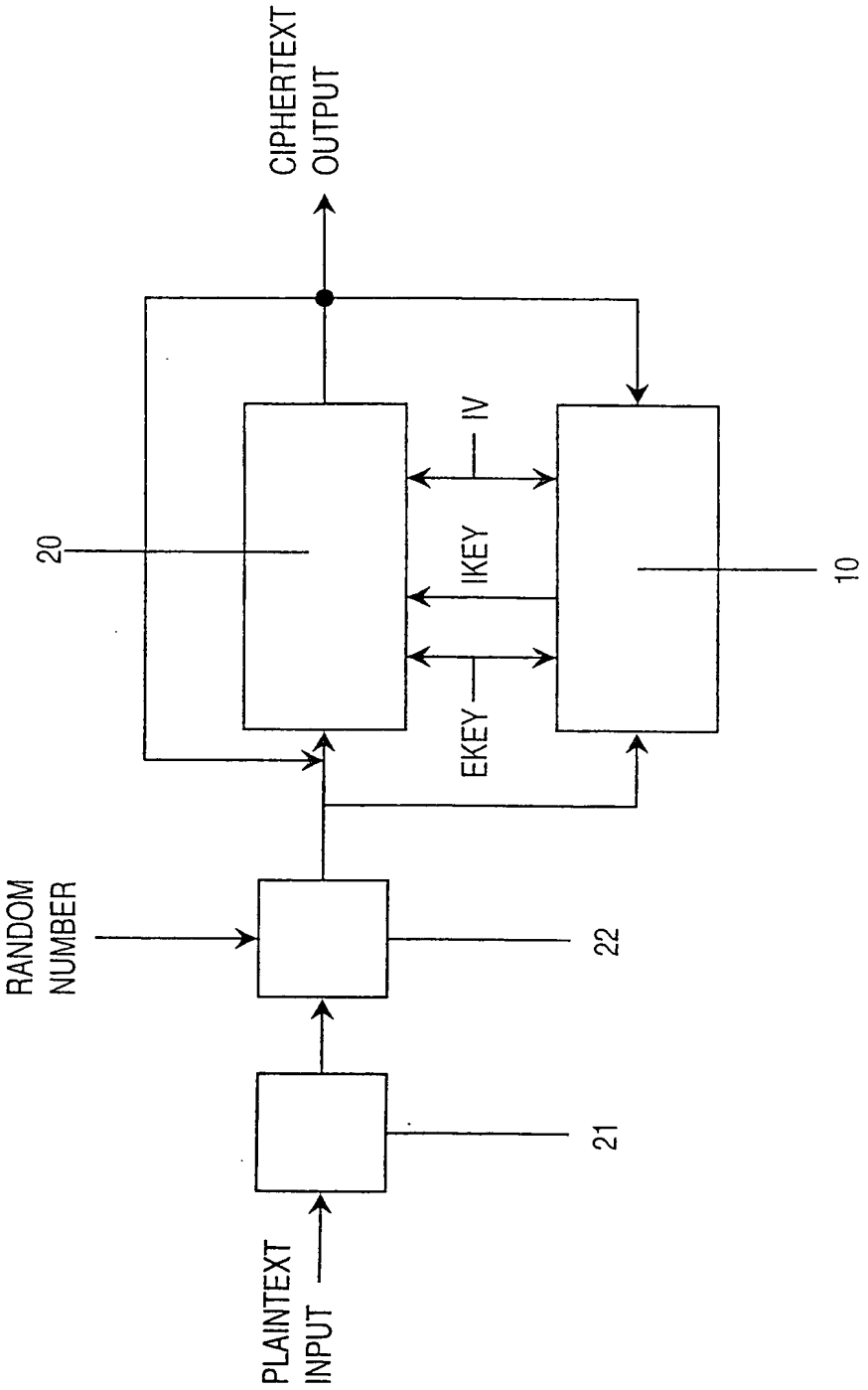
CIPHERTEXT
OUTPUT
IV
IKEY
EKEY
20
10
RANDOM
NUMBER
22
21
PLAINTEXT
INPUT

Fig.3

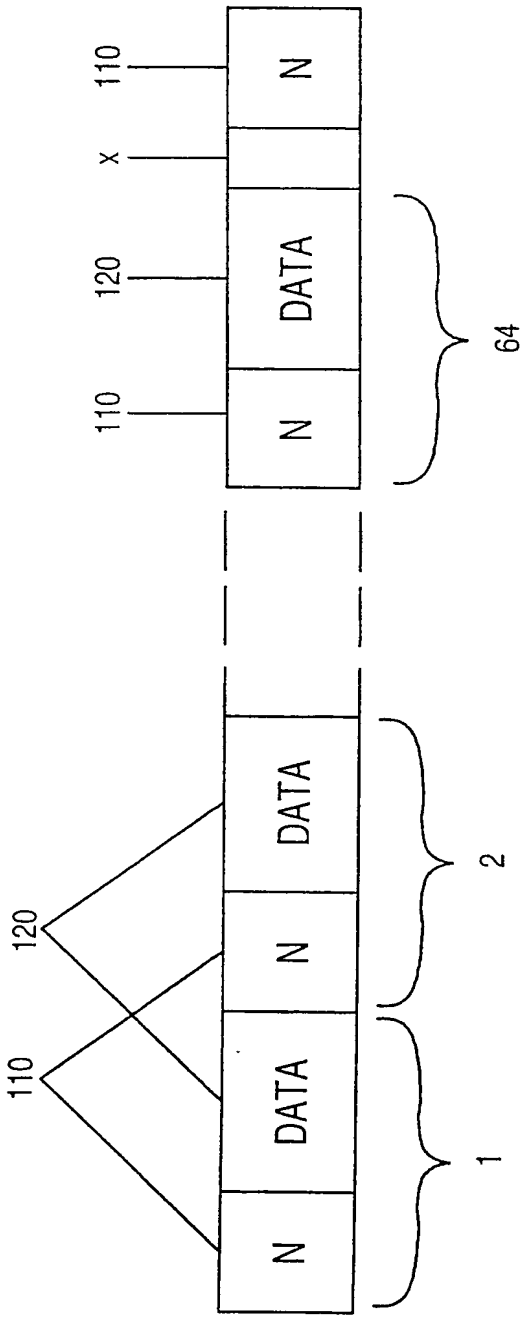

Fig.4

Fig.5

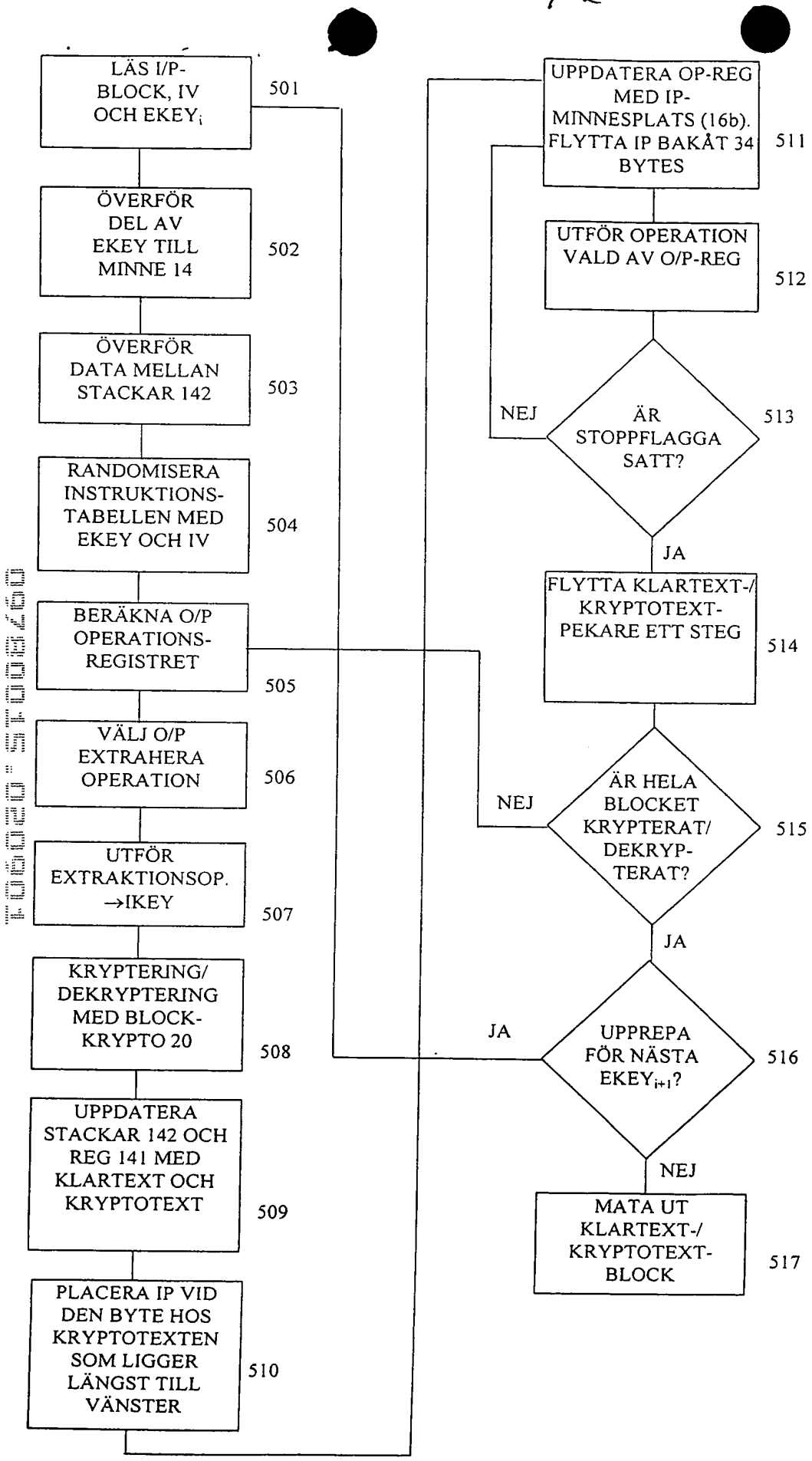
LÄS I/P-BLOCK, IV OCH EKEY$_i$
501
ÖVERFÖR DEL AV EKEY TILL MINNE 14
502
ÖVERFÖR DATA MELLAN STACKAR 142
503
RANDOMISERA INSTRUKTIONS-TABELLEN MED EKEY OCH IV
504
BERÄKNA O/P OPERATIONS-REGISTRET
505
VÄLJ O/P EXTRAHERA OPERATION
506
UTFÖR EXTRAKTIONSOP. →IKEY
507
KRYPTERING/ DEKRYPTERING MED BLOCK-KRYPTO 20
508
UPPDATERA STACKAR 142 OCH REG 141 MED KLARTEXT OCH KRYPTOTEXT
509
PLACERA IP VID DEN BYTE HOS KRYPTOTEXTEN SOM LIGGER LÄNGST TILL VÄNSTER
510
UPPDATERA OP-REG MED IP-MINNESPLATS (16b). FLYTTA IP BAKÅT 34 BYTES
511
UTFÖR OPERATION VALD AV O/P-REG
512
ÄR STOPPFLAGGA SATT?
513
NEJ
JA
FLYTTA KLARTEXT-/ KRYPTOTEXT-PEKARE ETT STEG
514
ÄR HELA BLOCKET KRYPTERAT/ DEKRYP-TERAT?
515
NEJ
JA
UPPREPA FÖR NÄSTA EKEY$_{i+1}$?
516
JA
NEJ
MATA UT KLARTEXT-/ KRYPTOTEXT-BLOCK
517

Fig.6

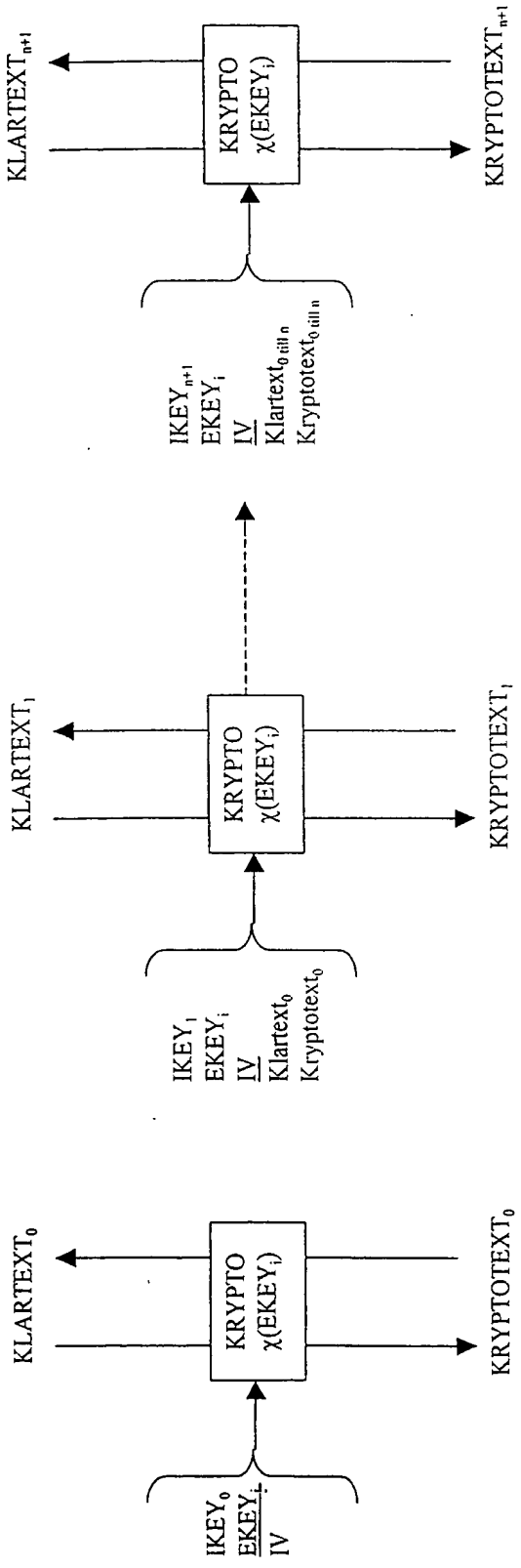
KLARTEXT$_{n+1}$
KRYPTO
χ(EKEY$_i$)
KRYPTOTEXT$_{n+1}$
IKEY$_{n+1}$
EKEY$_i$
IV
Klartext$_{0\ till\ n}$
Kryptotext$_{0\ till\ n}$
KLARTEXT$_1$
KRYPTO
χ(EKEY$_i$)
KRYPTOTEXT$_1$
IKEY$_1$
EKEY$_i$
IV
Klartext$_0$
Kryptotext$_0$
KLARTEXT$_0$
KRYPTO
χ(EKEY$_i$)
KRYPTOTEXT$_0$
IKEY$_0$
EKEY$_i$
IV

Fig.7

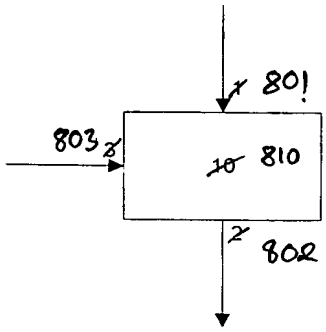

FIG. 8

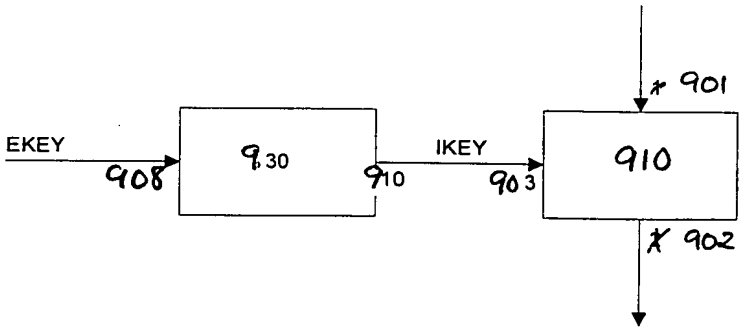

FIG. 9

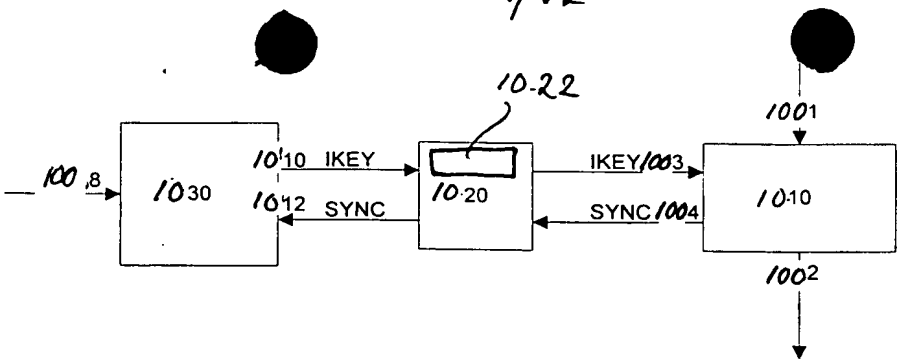

FIG. 10

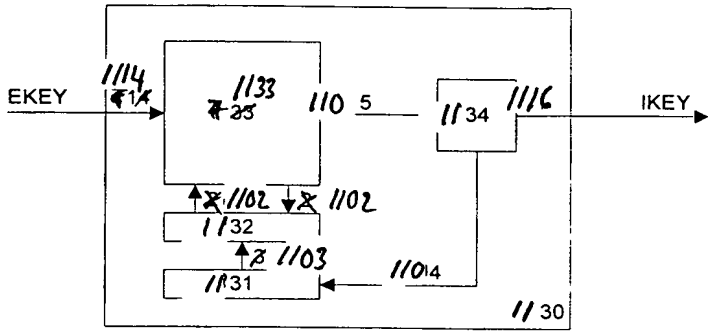

FIG. 11

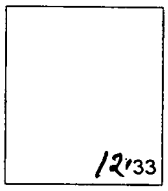

FIG. 12A

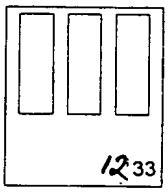

FIG. 12B

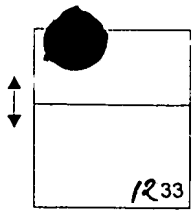

FIG.5c 12C

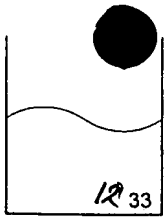

FIG.5d 12D

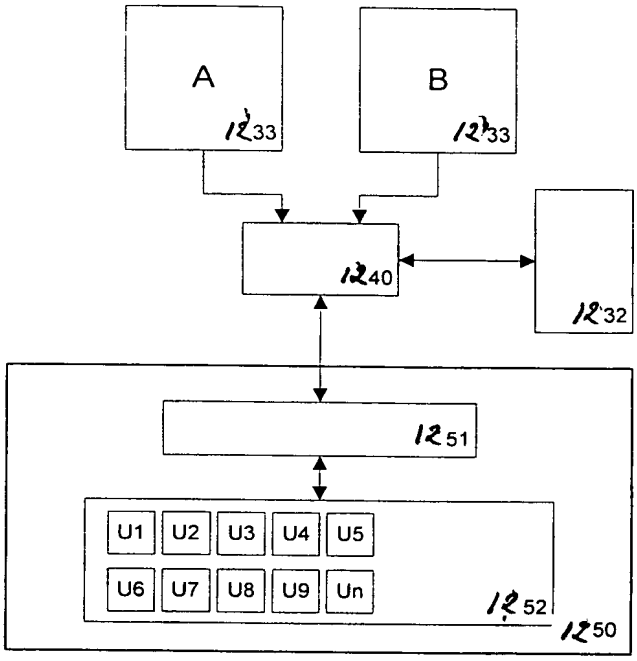

FIG.5e 12E

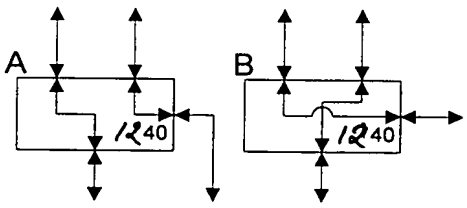

FIG.5f 12F

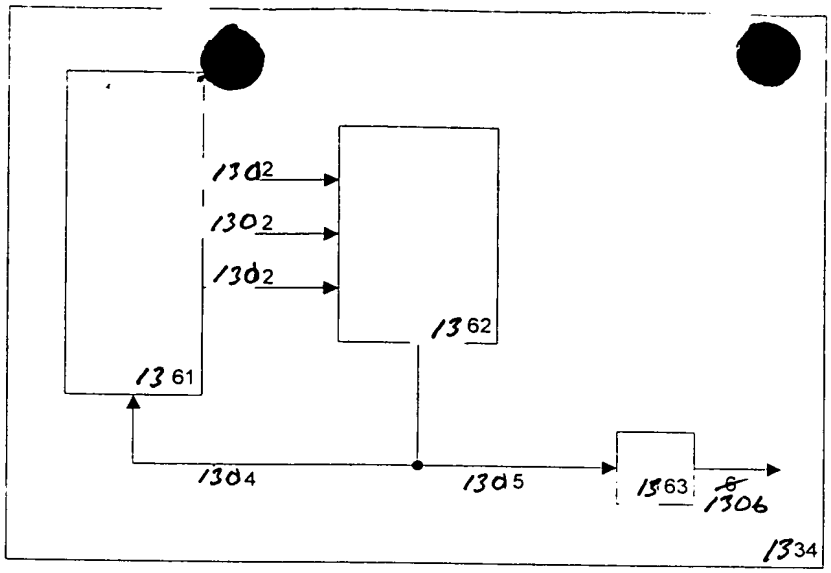

FIG. 13

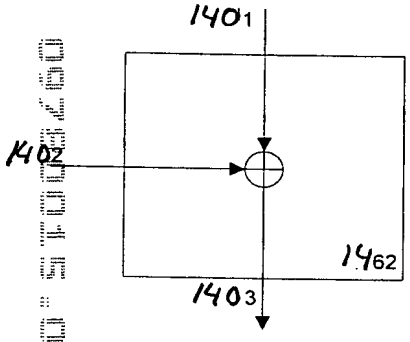

FIG. 14A

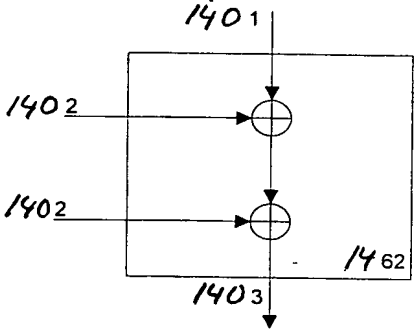

FIG. 14B

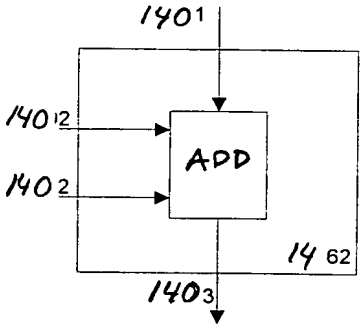

FIG. 14C

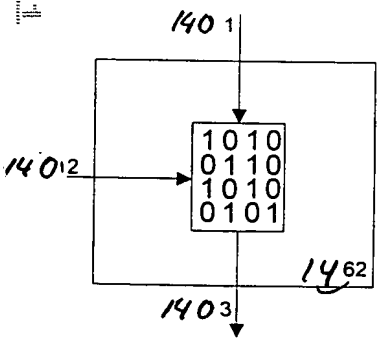

FIG. 14D

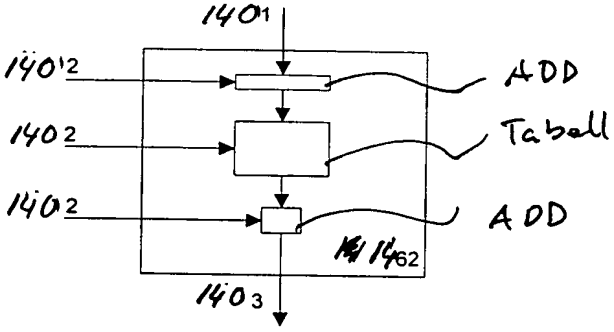

FIG. 14E

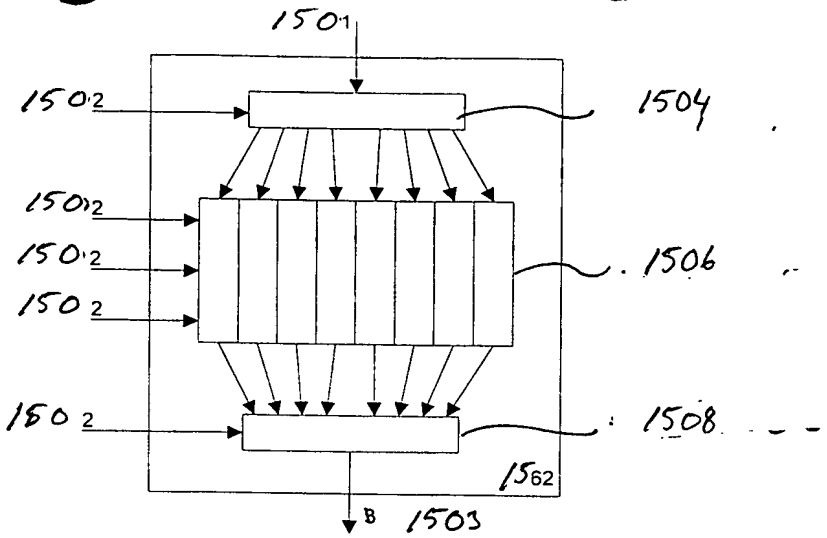

FIG. 8 15